Dr Artur Romaszewski
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych

Dr hab. med. Wojciech Trąbka
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych

Warunki i standardy dotyczące przetwarzania danych medycznych w nowych regulacjach unijnych.

Wstęp

Plan wprowadzenia w Unii Europejskiej nowych regulacji dotyczących ochrony danych osobowych wpłynie na standardy obowiązujących obecnie zasad przetwarzania danych osobowych a szczególnie danych o stanie zdrowia. Rozporządzenie UE przedefiniowało problem zgody pacjenta na przetwarzanie jego danych. Uregulowano zasady przechowywania i usuwania danych oraz zasady i prawa do informacji, poprawiania i usuwania lub prawa dostępu do danych i ich otrzymywania, prawa wniesienia sprzeciwu, profilowania, a także informowania podmiotu danych o naruszeniu ochrony danych osobowych. W artykule obok omówienia wpływu powyższych regulacji przedstawiono także problematykę planowanych zasad certyfikacji i akredytacji podmiotów przetwarzających dane osobowe. Oraz zunifikowane zasady przekazywania danych osobowych w krajach UE oraz poza jej obszar.

Zgoda podmiotu danych

W związku z tym, że najważniejszą przesłanką przy przetwarzaniu danych wrażliwych – w tym danych o stanie zdrowia - jest **zgoda podmiotu danych**, niezwykle istotne są podstawowe zasady dotyczące zgody.

Zgoda powinna być:

- wyraźnie wyrażona, w dowolny właściwy sposób umożliwiający swobodne i świadome wyrażenie woli przez podmiot danych bądź w formie oświadczenia,
- bądź w drodze wyraźnego działania potwierdzającego będącego konsekwencją wyboru dokonanego przez podmiot danych, przy jednoczesnym zagwarantowaniu, że osoby fizyczne są świadome, iż wyrażają zgodę na przetwarzanie danych osobowych.

Wyraźne działanie potwierdzające może polegać na zaznaczeniu okna wyboru podczas przeglądania strony internetowej lub też na innym oświadczeniu bądź zachowaniu, które w tym kontekście wyraźnie oznacza akceptację przez podmiot danych proponowanego przetwarzania jego danych osobowych. Milczenie, samo skorzystanie z usług i lub bezczynność nie powinny zatem stanowić zgody.

Zgoda powinna obejmować całość przetwarzania dokonanego w tym samym celu lub w tych samych celach. Jeśli zgoda podmiotu danych ma być wyrażona w następstwie elektronicznego wniosku, wniosek taki musi być jasny, zwięzły i nie powodować niepotrzebnego przerwania świadczenia usługi, której dotyczy[1].

Gdy przetwarzanie odbywa się na podstawie zgody, ciężar udowodnienia zgody podmiotu danych na przetwarzanie jego danych osobowych w określonych celach spoczywa na administratorze.

Jeśli zgoda podmiotu danych ma być udzielona w kontekście pisemnego oświadczenia, które dotyczy także innej kwestii, wymóg udzielenia zgody musi zostać przedstawiony w sposób pozwalający wyraźnie odróżnić go od tej innej kwestii.

Niezależnie od innych podstaw prawnych przetwarzania, podmiot danych ma prawo odwołać swoją zgodę w dowolnym momencie. Odwołanie zgody nie ma wpływu na zgodność z prawem przetwarzania opartego na zgodzie przed jej odwołaniem. Wycofanie zgody musi być równie łatwe jak jej udzielenie. Administrator informuje podmiot danych, jeżeli wycofanie zgody może skutkować zakończeniem świadczenia usług lub ustaniem relacji z administratorem.

Zgoda dotyczy konkretnego celu i traci ważność, gdy cel przestaje istnieć lub z chwilą, gdy przetwarzanie danych osobowych nie jest już potrzebne do realizacji celu, dla którego dane te zostały początkowo zgromadzone. Realizacja umowy lub świadczenie usługi nie może być uzależnione od zgody na przetwarzanie danych, które nie są niezbędne do realizacji umowy lub świadczenia usługi.

Każda osoba, której dane są przetwarzane, podobnie jak obecnie na mocy ustawy o ochronie danych osobowych, będzie miała zagwarantowane prawo:

[1] Poprawka 8 Wniosek dotyczący rozporządzenia Motyw 25 - Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

- dostępu do danych zebranych na jej temat, a wykonanie tego prawa powinno być na tyle łatwe, by każda osoba była świadoma przetwarzania i mogła zweryfikować jego zgodność z prawem. Dlatego też każdy podmiot danych powinien mieć prawo:
- do uzyskania wiadomości w szczególności o celach, dla których dane są przetwarzane,
- do wiedzy jaki jest szacowany okres przetwarzania,
- do informacji o odbiorcach otrzymujących dane,
- do informacji o ogólnych zasadach przetwarzania danych oraz ewentualnych skutkach tego przetwarzania. (przynajmniej w przypadku profilowania)

Każdy podmiot danych powinien ponadto mieć prawo do uzyskania informacji na temat danych osobowych podlegających przetwarzaniu oraz, na wniosek w formie elektronicznej, uzyskania kopii elektronicznej danych niehandlowych podlegających przetwarzaniu w formacie interoperacyjnym i zorganizowanym umożliwiającym dalsze wykorzystywanie.

Prawo to nie powinno negatywnie wpływać na prawa i wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, na przykład w odniesieniu do praw autorskich chroniących oprogramowanie. Powyżej omówione względy nie powinny jednak powodować odmowy udzielenia podmiotowi danych wszystkich informacji.

Każda osoba powinna mieć prawo do poprawienia dotyczących jej danych osobowych oraz „prawo do usunięcia danych", jeśli przechowywanie tych danych nie jest zgodne z Rozporządzeniem.

Przechowywanie i usuwanie danych osobowych

Podmiot danych ma prawo do tego, by jego dane osobowe zostały usunięte i nie były dalej przetwarzane:

- jeśli dane te nie są już konieczne do celów, dla których dane są zbierane lub przetwarzane w inny sposób,
- jeśli podmioty danych odwołały zgodę na przetwarzanie,
- jeśli wnoszą sprzeciw wobec przetwarzania danych osobowych ich dotyczących,
- lub jeśli przetwarzanie ich danych osobowych nie jest zgodne z rozporządzeniem z innego powodu.

Dalsze przechowywanie danych powinno być jednak dopuszczalne, jeśli jest ono niezbędne do celów dokumentacji, statystyki i badań naukowych, realizacji interesu publicznego w dziedzinie zdrowia publicznego, wykonania prawa wolności wypowiedzi, jeśli wymagają

tego przepisy prawa lub jeśli są powody ograniczenia przetwarzania danych zamiast ich usunięcia. Prawo do usunięcia danych nie ma również zastosowania, gdy zatrzymanie danych osobowych jest niezbędne w celu wykonania umowy z podmiotem danych lub gdy istnieje obwiązek prawny zatrzymania tych danych. W odniesieniu do danych o stanie zdrowia są Podmiot udzielający świadczeń zdrowotnych przechowuje dokumentację medyczną przez okres 20 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu, z wyjątkiem określonymi prawem[2].

„Prawo do usunięcia danych” w Internecie, powinno być także rozszerzone w taki sposób, by administrator, który upublicznił dane bez uzasadnienia prawnego, miał obowiązek poczynić wszelkie niezbędne kroki w celu doprowadzenia do usunięcia danych, w tym przez strony trzecie, bez uszczerbku dla przysługującego podmiotowi danych prawa do wystąpienia o odszkodowanie. Chodzi w tym przypadku o poinformowanie osób trzecich, które przetwarzają te dane, że podmiot przetwarzający dane złożył wniosek o usunięcie wszelkich linków do danych, kopii lub replikacji tych danych osobowych[3].

W przypadkach, w których dane osobowe mogłyby być przetwarzane zgodnie z prawem w celu ochrony żywotnych interesów podmiotu danych lub gdy jest to uzasadnione interesem publicznym, wykonywaniem władzy publicznej lub słusznymi interesami administratora, każdemu podmiotowi danych powinno jednak przysługiwać **prawo wniesienia sprzeciwu wobec przetwarzania danych go dotyczących** w prosty, skuteczny i wolny od opłat sposób. Ciężar dowodu w zakresie wykazania, że uzasadnione interesy administratora mogą mieć charakter nadrzędny wobec interesów lub podstawowych praw i wolności podmiotu danych, spoczywa na administratorze.

W przypadku kiedy podmiot danych ma prawo wniesienia sprzeciwu wobec przetwarzania, **administrator powinien wyraźnie poinformować o nim podmiot danych** w zrozumiały sposób i w zrozumiałej formie, jasnym i prostym językiem, oraz powinien wyraźnie wyodrębnić tę informację od innych informacji[4].

---

[2] Art. 29. 1 Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta Dz.U. 2009 nr 52 poz. 417

3 Poprawka Poprawka 27 Wniosek dotyczący rozporządzenia Motyw 53

4 Poprawka 31, 32 Wniosek dotyczący rozporządzenia Motyw 56, 57 Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

W praktyce często zdarza się, że podmiot leczniczy korzysta z usług dostarczających zarówno przestrzeni dyskowych, mocy obliczeniowych oraz kompleksowej usługi dostarczającej oprogramowania wraz z kompleksową obsługą zgromadzonych w procesie przetwarzania danych w tym danych o stanie zdrowia. Problemem staje się chęć zmiany usługodawcy zarówno wtedy kiedy zakończył się wiążący strony okres umowy jak i z powodu niezadowolenia strony ze świadczonej usługi. Teoretycznie podmiot może przenieść swoje dane do innego podmiotu świadczącego podobny zakres usług, w praktyce jednak często jest to niemożliwe ponieważ stosowane są różne formaty danych uniemożliwiające interoperacyjność. Przez interoperacyjność rozumie się to zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych[5]

W celu wzmocnienia kontroli nad własnymi danymi oraz prawa dostępu, podmioty danych powinny mieć prawo, w przypadku gdy dane osobowe są przetwarzane w sposób elektroniczny oraz w zorganizowanym i powszechnie używanym formacie, do otrzymania kopii dotyczących ich danych także w takim powszechnie używanym formacie elektronicznym. Podmiot danych powinien także móc przekazywać dane, które dostarczył, ze zautomatyzowanej aplikacji, takiej jak sieć społeczna, do innej. Administratorów danych należy zachęcać do opracowywania interoperacyjnych formatów umożliwiających przenoszenie danych. Powinno to mieć zastosowanie wtedy, gdy podmiot danych dostarczył dane do automatycznego systemu przetwarzania na podstawie swojej zgody lub w związku z wykonaniem umowy. Dostawcy usług społeczeństwa informacyjnego nie powinni uzależniać świadczenia swoich usług od przekazywania tych danych[6.]

Profilowanie

Coraz częściej zdarza się, że różnego rodzaju instytucje z sektora finansowego, np. banki czy ubezpieczyciele, ale także firmy marketingowe, z różnych źródeł pozyskują dane

5 Art. 3 18) Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne Dz.U. 2005 nr 64 poz. 565
6 Poprawka 30 Wniosek dotyczący rozporządzenia
Motyw 55

osobowe, które były zebrane zgodnie z prawem dla określonego celu, i dołączają je do innych danych o swoich klientach, tworząc tzw. profil osobowościowy. Zgodnie z Rozporządzeniem „profilowanie" oznacza wszelką formę automatycznego przetwarzania danych mającego służyć ocenie niektórych aspektów osobistych tej osoby fizycznej lub też analizie bądź przewidzeniu zwłaszcza wyników w pracy, sytuacji ekonomicznej, miejsca przebywania, zdrowia, preferencji osobistych, wiarygodności lub zachowania tej osoby fizycznej[7].

Profilowanie może przybierać dwie formy. – Pierwszą formą jest tworzenie profilu konkretnej osoby na potrzeby działalności marketingowej bądź przygotowywania oferty dla klienta albo oceny jego zdolności co do ponoszenia pewnego rodzaju obciążeń. Drugą formą jest przypisywanie do takiego zestawu danych pewnych dodatkowych profili, które statystycznie się sprawdzają. Czyli jeżeli osoba wykazuje jakąś cechę A, to statystycznie powinna wykazywać również cechę B i C . Inaczej mówiąc, do danych, które są w jakimś stopniu obiektywne, ponieważ albo zostały zebrane zgodnie z prawem, albo przekazane przez osobę, której dotyczą, dołącza się dane, które statystycznie powinny się w stosunku do niej sprawdzać.

GIODO wskazywał, że w ten sposób zmienia się cel przetwarzania danych, a ponadto tworzy zestaw nowych danych osobowych, innych niż te, które sama osoba, której dane dotyczą, podała administratorowi lub których znajomości przez administratora w uzasadniony sposób może się spodziewać. [8.]

Można przyjąć, że w zakresie szeroko pojętej ochrony zdrowia mechanizm ten może być wykorzystywany np. na podstawie zapytań o lek lub schorzenie osoba zadająca pytanie będzie otrzymywała odpowiednio dostosowaną reklamę leków lub podmiotów udzielających określonych usług z zakresu świadczenia usług medycznych

W związku z tymi zagrożeniami przyjęto, że profilowanie, które prowadzi do środków wywołujących skutki prawne dotyczące podmiotu danych lub ma podobnie istotny wpływ na interesy, prawa lub wolności tego podmiotu danych, powinno być dozwolone jedynie wtedy, gdy jest:

- wyraźnie przewidziane przez przepisy prawa,
- stosowane w toku zawierania lub wykonywania umowy

7 3a) art. 4 Poprawka 98 Wniosek dotyczący rozporządzenia Artykuł 4
8 PROFILOWANIE TO ODRĘBNY CEL PRZETWARZANIA DANYCH OSOBOWYCH, 25.05.2011 R. http://www.giodo.gov.pl/1520098/id_art/4151/j/pl/

- lub gdy podmiot danych wyraził na nie zgodę.

W każdym przypadku takie przetwarzanie powinno stanowić przedmiot odpowiednich gwarancji, w tym konkretnych informacji podmiotu danych i prawa do oceny ze strony człowieka, a środek ten nie powinien dotyczyć dzieci. Takie środki nie powinny prowadzić do dyskryminacji osób ze względu na rasę lub pochodzenie etniczne, poglądy polityczne, religię lub przekonania, członkostwo w związkach zawodowych, orientację seksualną lub tożsamość płciową.[9]

Każda osoba fizyczna powinna mieć prawo do sprzeciwu wobec profilowania, Bez uszczerbku dla zgodności przetwarzania danych z prawem

Należy zakładać, że profilowanie oparte wyłącznie na przetwarzaniu danych pseudonimicznych nie ma istotnego wpływu na interesy, prawa lub wolności podmiotu danych. Gdy profilowanie – niezależnie od tego, czy jest oparte na pojedynczym źródle danych pseudonimicznych, czy też na agregacji danych pseudonimicznych z różnych źródeł – umożliwia administratorowi przypisanie danych pseudonimicznych do konkretnego podmiotu danych, przetwarzane dane nie mogą już być uznawane za pseudonimiczne[10].

Ograniczenia dotyczące szczególnych zasad i praw mogą być nałożone przez prawo Unii lub państwa członkowskiego w zakresie, w jakim jest to konieczne i proporcjonalne w demokratycznym społeczeństwie, by zagwarantować bezpieczeństwo publiczne, w tym ochronę życia ludzkiego, zwłaszcza w ramach reagowania na klęski żywiołowe lub katastrofy wywołane przez człowieka, możliwość zapobiegania przestępstwom lub naruszeniom zasad etyki w przypadku zawodów regulowanych, ich ścigania i karania, inne szczególne i dobrze zdefiniowane publiczne interesy Unii lub państwa członkowskiego.

---

9 Poprawka 33 Wniosek dotyczący rozporządzenia Motyw 58 Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

10 Poprawka 34 Wniosek dotyczący rozporządzenia Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

Motyw 58 a (nowy) Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

Potrzeba rozwiązań systemowych w opiece zdrowotnej – certyfikacja, akredytacja

Administrator przyjmuje odpowiednie zasady i realizuje odpowiednie i możliwe do wykazania środki techniczne i organizacyjne, aby zapewnić, by przetwarzanie danych osobowych odbywało się zgodnie z Rozporządzeniem, oraz być w stanie wykazać tę zgodność w przejrzysty sposób, uwzględniając najnowsze osiągnięcia techniczne, charakter przetwarzania danych osobowych, kontekst, zakres i cele przetwarzania, ryzyko dla praw i wolności podmiotów danych oraz rodzaj organizacji, zarówno podczas określania sposobów przetwarzania, jak i podczas samego przetwarzania. Uwzględniając najnowsze osiągnięcia techniczne oraz koszty wdrożenia, administrator podejmuje wszelkie racjonalne kroki w celu wdrożenia zasad i procedur zgodności, które stale respektują niezależne wybory dokonane przez podmioty danych. Te zasady zgodności są poddawane przeglądowi co najmniej co dwa lata i w razie konieczności aktualizowane[11].

W obecnym stanie prawnym brakuje przepisów dotyczących certyfikacji rozwiązań zapewniających bezpieczeństwo danych m.in. w podmiotach leczniczych. Powoduje to, że zastosowane rozwiązania mogą być poddawane ocenie intuicyjnej, bez wyraźnie ustanowionych standardów do których można się odnieść. Powoduje to, że podmiot danych nie jest w stanie obiektywnie stwierdzić, że jego dane osobowe przetwarzane w konkretnej instytucji np. świadczące usługi zdrowotne, są bezpieczne.

W celu zmiany tej sytuacji należy:

- zachęcać zrzeszenia lub inne organy reprezentujące różne kategorie administratorów do sporządzenia kodeksów postępowania, Kodeksy takie powinny ułatwić branży zachowanie zgodności z przepisami[12].

11 Poprawka 117 Wniosek dotyczący rozporządzenia Artykuł 22 Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

12 Poprawka 51 Wniosek dotyczący rozporządzenia Motyw 76 Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

- Zachęcać państwa członkowskie UE do ustanowienia mechanizmów certyfikacji oraz wprowadzenia pieczęci i standaryzowanych oznaczeń w zakresie ochrony danych, umożliwiając w ten sposób podmiotom danych szybką, wiarygodną i weryfikowalną ocenę poziomu ochrony danych odnośnych produktów i usług[13].
- Należy ustanowić „europejską pieczęć w zakresie ochrony danych" na szczeblu europejskim, aby zapewnić zaufanie wśród podmiotów danych, pewność prawa dla administratorów, a jednocześnie promować europejskie standardy ochrony danych poza UE przez ułatwienie pozaeuropejskim przedsiębiorstwom dostępu do rynków europejskich po przejściu procedury certyfikacji.

Dowolny administrator lub podmiot przetwarzający może zwrócić się do dowolnego organu nadzorczego w Unii, za racjonalną opłatą uwzględniającą koszty administracyjne, o poświadczenie, że przetwarzanie danych osobowych odbywa się zgodnie z niniejszym rozporządzeniem, w szczególności z zasadami dotyczące przetwarzania danych osobowych oraz zasadami zapewniającymi bezpieczeństwo przetwarzania.

Akredytować będzie można również audytorów działających z ramienia wyspecjalizowanych firm do przeprowadzenia w ich imieniu kontroli administratora lub podmiotu przetwarzającego. Tacy audytorzy działający z ramienia stron trzecich mają wykwalifikowany personel oraz są bezstronni i wolni od wszelkich konfliktów interesów w odniesieniu do swoich obowiązków. Organy nadzorcze przyznają administratorom i podmiotom przetwarzającym, co do których w wyniku audytu poświadczono, że przetwarzają dane osobowe zgodnie z niniejszym rozporządzeniem, standardowe oznaczenie w zakresie ochrony danych nazywane „europejską pieczęcią w zakresie ochrony danych".

Europejska pieczęć w zakresie ochrony danych jest ważna tak długo, jak długo operacja przetwarzania danych prowadzone przez akredytowanego administratora lub podmiot przetwarzający są w pełni zgodne z rozporządzeniem. Zakłada się że certyfikacja jest ważna najwyżej przez pięć lat. Europejska Rada Ochrony Danych ustanawia publiczny rejestr elektroniczny, zawierający wykazy ważnych i nieważnych certyfikatów wydanych w państwach członkowskich.

13 Poprawka 52 Wniosek dotyczący rozporządzenia Motyw 77 Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

Europejska Rada Ochrony Danych może z własnej inicjatywy poświadczyć, że standard techniczny służący wzmocnieniu ochrony danych jest zgodny z Rozporządzeniem

Zakłada się, że komisja jest uprawniona do przyjmowania – po zasięgnięciu opinii Europejskiej Rady Ochrony Danych aktów delegowanych , w celu doprecyzowania kryteriów i wymogów dotyczących mechanizmów certyfikacji w zakresie ochrony danych, audytorów, warunków przyznawania i odwoływania, oraz wymogów w zakresie uznawania i promowania na terytorium Unii i w państwach trzecich. Takie akty delegowane przyznają podmiotom danych egzekwowalne prawa[14].

Przekazywanie danych medycznych poza granice UE

W Unii Europejskiej przestrzegana jest zasada, że dozwolone jest przekazywanie danych osobowych na terenie Unii Europejskiej bez żadnych dodatkowych zezwoleń. Problem pojawia się kiedy dane przekazywane są do państwa spoza Europejskiego Obszaru Gospodarczego. Problem wraz ze zwiększoną emigracją oraz planowanym zniesieniem wiz do USA może być bardzo znaczący w sektorze ochrony zdrowia. Osoby zmieniające stałe miejsce zamieszkania będą potrzebowały bądź stałego dostępu do danych znajdujących się w Polsce bądź jednorazowego przeniesienia danych. Dużym problemem jest również przechowywanie danych w chmurach obliczeniowych w dużej mierze należących do amerykańskich podmiotów gospodarczych, a więc takich, które nie zapewniają odpowiedniej ochrony danym osobowym.

Zasadą jest w takim przypadku, tj. gdy państwo trzecie, do którego przekazywane są dane osobowe nie zapewnia na swoim terytorium odpowiedniego poziomu ochrony danych osobowych, że administrator danych osobowych powinien uzyskać zgodę organu nadzorczego w formie decyzji. Zgoda taka jest wydawana pod warunkiem, że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą.

Zgoda nie jest wymagana w przypadku , gdy:

14 Poprawka 135 Wniosek dotyczący rozporządzenia Artykuł 38 Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

- ✓ osoba, której dane dotyczą, udzieliła na to zgody na piśmie;
- ✓ przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie;
- ✓ przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem;
- ✓ przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych;
- ✓ przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą;
- ✓ dane są ogólnie dostępne.

W innych przypadkach, niż wskazane powyżej, zgoda GIODO nie będzie wymagana, o ile administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą, przez:

- standardowe klauzule umowne ochrony danych osobowych, zatwierdzone przez Komisję Europejską[15] lub
- prawnie wiążące reguły tzw. wiążącymi regułami korporacyjnymi lub polityki ochrony danych osobowych, które zostały zatwierdzone przez Generalnego Inspektora[16]. Zgodnie z Rozporządzeniem wiążące reguły korporacyjne oznaczają zasady ochrony danych osobowych, których przestrzegają administrator lub podmiot przetwarzający mający siedzibę na terytorium państwa członkowskiego Unii do celów przekazywania danych osobowych do administratora lub podmiotu przetwarzającego w przynajmniej jednym państwie trzecim w ramach grupy przedsiębiorstw[17].

15 zgodnie z art. 26 ust. 4 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995, str. 31, z późn. zm.; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, str. 355, z późn. zm.)

16 Rozwiązanie dotyczące wiążących reguł korporacyjnych jest wyłącznie inkorporowaniem do polskiego porządku prawnego zasad obowiązujących już w GIODO po wprowadzenia w dniu 1 stycznia 2013 r. wiążących reguł korporacyjnych (BCR) dla przetwarzających stworzonych przez Grupę Roboczą Artykułu 29 ds. Ochrony Danych.

17) Poprawka 98 Wniosek dotyczący rozporządzenia Artykuł 4 Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

Administrator ma prawo do przekazywania danych osobowych w obrębie Unii w ramach grupy przedsiębiorstw, której administrator jest częścią, gdy takie przetwarzanie jest niezbędne ze względu na uzasadnione administracyjne cele wewnętrzne między powiązanymi obszarami biznesowymi grupy przedsiębiorstw oraz gdy odpowiedni poziom ochrony danych, a także interesy podmiotów danych są zabezpieczone wewnętrznymi przepisami dotyczącymi ochrony danych lub równoważnymi kodeksami postępowania Zatwierdzenie przez organ nadzorczy wiążących reguł korporacyjnych oznacza , że wszyscy administratorzy danych należący do określonej korporacji będą mogli przekazywać między sobą dane osobowe bez uzyskiwania zgody GIODO. Ma to istotne znaczenie w przypadku międzynarodowych podmiotów przetwarzających dane w ramach umowy powierzenia. Zgodnie z Rozporządzeniem Właściwy organ nadzorczy zatwierdza w ramach pojedynczego zatwierdzenia wiążące reguły korporacyjne dla grupy przedsiębiorstw. Reguły te pozwolą na wielokrotne międzynarodowe przekazywanie danych w obrębie Europy i poza nią w ramach tej grupy, pod warunkiem że: są one prawnie wiążące i mają zastosowanie do oraz są egzekwowane przez wszystkich członków grupy przedsiębiorstw administratora lub podmiotu przetwarzającego i ich podwykonawców zewnętrznych, i obejmują ich pracowników. wyraźnie przyznają podmiotom danych egzekwowalne prawa i są przejrzyste dla podmiotów danych.

W ramach usług chmury obliczeniowej dostawcy usług przetwarzania w chmurze często korzystają z usług podwykonawców zewnętrznych w celu wykonania konkretnego zadania oraz zapewnienia całodobowego utrzymania i obsługi przez siedem dni w tygodniu. Powinno to znaleźć odzwierciedlenie w wiążących regułach korporacyjnych organu nadzorczego[18].

Standardowe klauzule umowne zatwierdzane przez Komisję Europejską są umową między administratorem danych osobowych przekazującym dane osobowe (eksporterem), a

18 Poprawka 312 Wniosek dotyczący rozporządzenia Artykuł 43 – ustęp 1 – litera a Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

podmiotem/podmiotami je otrzymującym/mi (importerem)[19]. Obecnie funkcjonują dwa wzory standardowych klauzuli umownych, które stanowią:

1) załącznik do Decyzji Komisji z 5 lutego 2010 roku (powierzenie) w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46WE Parlamentu Europejskiego i Rady

2) załącznik do Decyzji Komisji (udostępnienie) z dnia 27 grudnia 2004 r. zmieniającej decyzję 2001/497/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich (notyfikowana jako dokument nr K(2004) 5271).

Umowa składa się z informacji o podmiocie przekazującym i odbierającym dane osobowe oraz zawiera w swojej treści zapisy zapewniające odpowiedni poziom ochrony danych osobowych, są to m.in.: klauzula na rzecz osoby trzeciej, obowiązki przekazującego dane, obowiązki odbierającego dane, odpowiedzialność, prawo właściwe, podwykonawstwo przetwarzania danych, obowiązki po zakończeniu usług przetwarzania danych osobowych. Do standardowych klauzul umownych dołączone są dwa dodatki:

1) pierwszy dotyczy szczegółowych informacji dotyczących podmiotu przekazującego i odbierającego dane, osób, których dane dotyczą, kategorie danych, czynności przetwarzania,

2) drugi dotyczy opisu technicznych i organizacyjnych środków bezpieczeństwa, które podmiot odbierający dane wdrożył[20].

Administrator lub podmiot przetwarzający mogą przekazywać dane osobowe do państwa trzeciego lub organizacji międzynarodowej do celów dokumentacji, statystycznych lub naukowych, jeżeli:

a) celów tych nie można inaczej osiągnąć w drodze przetwarzania danych, które nie umożliwia lub przestaje umożliwiać identyfikację osoby, której dane dotyczą;

19 których mowa w art. 26 ust. 2 Dyrektywy, 95/46/WE PARLAMENTU EUROPEJSKIEGO I RADY z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych

20 STANDARDOWE KLAUZULE UMOWNE, WIĄŻĄCE REGUŁY KORPORACYJNE - JAKIE MAJĄ ZNACZENIE DLA PRZETWARZANIA DANYCH OSOBOWYCH? – portal E-ochronadanych.pl ttp://www.e-ochronadanych.pl/przekazywanie_danych_osobowych_do_panstwa_trzeciego.php?news_id=2455

b) odbiorca nie ma z rozsądnym prawdopodobieństwem dostępu do danych, które pozwalają na przypisanie informacji do zidentyfikowanego lub możliwego do zidentyfikowania podmiotu danych; oraz

c) klauzule umowne podpisane między administratorem lub podmiotem przetwarzającym a odbiorcą danych uniemożliwiają ponowną identyfikację podmiotu danych i ograniczają przetwarzanie danych zgodnie z warunkami i gwarancjami określonymi w tym artykule.

Odbiorca danych kodowanych kluczem i przekazywanych do celów badań naukowych nie ma możliwości ponownego zidentyfikowania podmiotów danych, a na mocy niniejszej poprawki nie ma również dostępu do klucza i umownie zabrania mu się dokonywać ponownej identyfikacji podmiotów danych. Niniejsza poprawka pozwala sformalizować proces zapewnienia z rozsądnym prawdopodobieństwem, że dane kodowane kluczem nie zostaną ponownie zidentyfikowane przez odbiorców mających siedzibę w państwach trzecich, co umożliwi przekazywanie takich danych bez dalszych obciążeń.

Literatura

1. Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta Dz.U. 2009 nr 52 poz. 417
2. ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)
3. Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)
4. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 1997 nr 133 poz. 883
5. DYREKTYWA 95/46/WE PARLAMENTU EUROPEJSKIEGO I RADY z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych
6. STANDARDOWE KLAUZULE UMOWNE, WIĄŻĄCE REGUŁY KORPORACYJNE - JAKIE MAJĄ ZNACZENIE DLA PRZETWARZANIA DANYCH OSOBOWYCH? – portal E-ochronadanych.pl
7. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 1997 nr 133 poz. 883 Strona Unii Europejskiej http://europa.eu/eu-law/decision-making/legal-acts/index_pl.htm
8. Komisja Europejska Memo http://europa.eu/rapid/press-release_MEMO-14-186_pl.htm

9. J.Bardadyn Kiedy (ostatecznie!) i jak UE zreformuje prawo ochrony danych osobowych? http://blog-daneosobowe.pl/ue-ostatecznie-zreformuje-prawo-ochronie-danych-osobowych-beda-kluczowe-zalozenia/
10. PROFILOWANIE TO ODRĘBNY CEL PRZETWARZANIA DANYCH OSOBOWYCH, 25.05.2011 R. http://www.giodo.gov.pl/1520098/id_art/4151/j/pl/
11. M. Chmielecki UNIJNA REFORMA PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH - INFORMACJE OGÓLNE e-ochronadanych.pl http://www.e-ochronadanych.pl/regulamin.php
12. M. Cwener PROPOZYCJE ZMIAN W ZAKRESIE PRZEPISÓW DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH – CZ. I; ii OGÓLNE e-ochronadanych.pl http://www.e-ochronadanych.pl/regulamin.php
13. K. Szymielewicz Półprzepuszczalny standard ochrony danych https://panoptykon.org/wiadomosc/polprzepuszczalny-standard-ochrony-danych
14. K.Witkowska Reforma ochrony danych osobowych - nowe obowiązki, nowe korzyści https://www.portalodo.com/entry/reforma-ochrony-danych-osobowych-nowe-obowiazki-nowe-korzysci.
15. P. Wierzbicki Jest szansa na unijne rozporządzenie o ochronie danych (2014.02.11) Obserwator Konstytucyjny http://www.obserwatorkonstytucyjny.pl/debaty/jest-szansa-na-unijne-rozporzadzenie-o-ochronie-danych/

Streszczenie

Plan wprowadzenia w Unii Europejskiej nowych regulacji dotyczących ochrony danych osobowych wpłynie na standardy obowiązujących obecnie zasad przetwarzania danych osobowych w szczególnie danych o stanie zdrowia. Rozporządzenie UE przedefiniowało problem zgody pacjenta na przetwarzanie jego danych. Uregulowano zasady przechowywania i usuwania danych oraz zasady i prawa do informacji, poprawiania i usuwania lub prawa dostępu do danych i ich otrzymywania, prawa wniesienia sprzeciwu, profilowania, a także informowania podmiotu danych o naruszeniu ochrony danych osobowych. W artykule obok omówienia wpływu powyższych regulacji przedstawiono także problematykę planowanych zasad certyfikacji i akredytacji podmiotów przetwarzających dane osobowe. Oraz zunifikowane zasady przekazywania danych osobowych w krajach UE oraz poza jej obszar.